BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of: Goodman et al.	:	Before the Examiner: Chai, Longbit
Serial No.: 09/931,629	:	Group Art Unit: 2131
Filing Date: August 16, 2001	:	
Title: FLASH UPDATE USING A TRUSTED PLATFORM MODULE	:	Lenovo (United States) Inc. Building 675, Mail C-137 4401 Silicon Drive Durham, NC 27709

SUPPLEMENTAL APPEAL BRIEF

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

I. REAL PARTY IN INTEREST

The real party in interest is Lenovo (Singapore) Pte. Ltd., which is the assignee of the entire right, title and interest in the above-identified patent application.

II. RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to Appellants, Appellants' legal representative or assignee which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal, except that Appellants filed an appeal of the rejections of the claims in U.S. Patent Application Serial No. 09/931,550, which is the subject of the provisional double patenting rejection in this Application.

III. STATUS OF CLAIMS

Claims 1-4 and 6-10 are pending in the Application. Claim 5 was cancelled. Claims 1-4 and 6-10 stand rejected. Claims 1-4 and 6-10 are appealed.

IV. STATUS OF AMENDMENTS

Appellants have not submitted any amendments following receipt of the final rejection with a mailing date of September 20, 2005.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Independent Claim 1:

In one embodiment of the present invention, a method for updating a program in a data processing system comprising the step of requesting a trusted platform module ("TPM") to perform a signature verification of an update to the program. Specification, page 9, lines 7-9; Figure 1, step 101. The method further comprises the TPM performing the signature verification of the update to the program. Specification, page 9, lines 9-11; Figure 2, step 201. Additionally, the method comprises that if the signature verification of the update to the program is successful, using the TPM for unlocking a memory unit storing the program. Specification, page 10, lines 6-8; Figure 2, step 203. Further, the method comprises modifying the program with the update to the program in response to the unlocking of the memory unit storing the program. Specification, page 10, lines 14-15; Figure 1, step 106.

Independent Claim 4:

In one embodiment of the present invention, a computer program product for storage on a computer readable medium and operable for updating a BIOS stored in a flash memory in a data processing system, comprises a BIOS update application program receiving an updated BIOS image. Specification, page 7, line 20 – page 8, line 5; Specification, page 9, lines 3-9; Figure 1, step 101. The computer program product further comprises the BIOS update application requesting a TPM to perform

a signature verification of the updated BIOS image. Specification, page 7, line 20 – page 8, line 5; Specification, page 9, lines 6-9; Figure 1, step 101. Additionally, the computer program product comprises a TPM program receiving the request from the BIOS update application to perform the signature verification of the updated BIOS image. Specification, page 7, line 20 – page 8, line 5; Specification, page 9, lines 9-11; Figure 2, step 201. Furthermore, the computer program product comprises the TPM program performing the signature verification of the updated BIOS image and posting a result of the signature verification of the updated BIOS image to the BIOS update application. Specification, page 7, line 20 – page 8, line 5; Specification, page 9, lines 9-13; Specification, page 10, lines 2-5; Specification, page 10, lines 9-10; Figure 2, steps 201, 204. Further, the computer program product comprises that if the result of the signature verification of the updated BIOS image determines that the updated BIOS image is authentic, then the TPM program unlocks the flash memory. Specification, page 7, line 20 – page 8, line 5; Specification, page 10, lines 6-8; Figure 2, steps 202, 203. Additionally, the computer program product comprises the BIOS update application modifies the BIOS with the updated BIOS image. Specification, page 7, line 20 – page 8, line 5; Specification, page 10, lines 14-15; Figure 1, step 106.

Independent Claim 8:

In one embodiment of the present invention, a data processing system having circuitry for updating a BIOS stored in a flash memory in the data processing system, comprising input circuitry for receiving an updated BIOS image. Specification, page 9, lines 3-9; Figure 1, step 101; Figure 3, element 313. The system further comprises circuitry for requesting a TPM to perform a signature verification of the updated BIOS image. Specification, page 9, lines 6-9; Figure 1, step 101. Additionally, the system comprises the TPM performing the signature verification of the updated BIOS image. Specification, page 9, lines 9-11; Figure 2, step 201. Furthermore, the system comprises the TPM unlocking the flash memory if the signature verification of the updated BIOS image determines that the updated BIOS image is authentic.

Specification, page 10, lines 6-8; Figure 2, steps 202, 203. Further, the system comprises circuitry for modifying the BIOS with the updated BIOS image. Specification, page 10, lines 14-15; Figure 1, step 106.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. Claims 1, 4 and 8 stand provisionally rejected under the judicial created doctrine of obviousness-type double patenting as being unpatentable over claim 18 (and claim 3) of co-pending Application Serial No. 09/931,550.

B. Claims 1-4 and 6-10 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Alexander et al. (U.S. Patent No. 6,188,602) (hereinafter "Alexander") in view of Grawrock (U.S. Patent No. 6,678,833).

VII. ARGUMENT

A. Addressing Provisional Obviousness-Type Double Patenting Rejection.

Claims 1, 4 and 8 stand provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 18 (and claim 3) of co-pending Application Serial No. 09/931,550. In response, Appellants respectfully traverse this rejection, however, since the co-pending application is merely pending, Appellants will address this double patenting rejection when either such co-pending application issues or claims 1, 4 and 8 are allowed in this Application.

B. Claims 1-4 and 6-10 are not properly rejected under 35 U.S.C. §103(a).

Claims 1-4 and 6-10 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Alexander in view of Grawrock. In response, Appellants respectfully traverse these rejections for at least the reasons stated below.

1. Claims 1, 4 and 8 are patentable over Alexander in view of Grawrock.

Claim 1 recites that a TPM performs a signature verification of an update to a program. Claim 1 further recites that if this signature verification is successful, then the TPM unlocks a memory unit to store the program. Claim 1 additionally recites modifying the program with the update to the program in response to the unlocking of the memory unit storing the program. Claims 4 and 8 similarly recite that a TPM performs a signature verification of an update to a program, such as a BIOS image. Claims 4 and 8 further recite that if this signature verification is successful, then the TPM unlocks a memory unit to store the program. Additionally, claims 4 and 8 recite that if the result of the signature verification of the updated BIOS image determines that the updated BIOS image is authentic, then the TPM program unlocks the flash memory and the BIOS update application modifies the BIOS with the updated BIOS image.

The Examiner asserts that the combination of Grawrock and Alexander teaches the above-cited claim limitations. Appellants had previously filed a declaration under 37 C.F.R. §1.132 by Steve Goodman, Randall F. Springfield and James Hoff, who are the inventors of the present application, on February 14, 2005 (hereinafter "Declaration 1"). Steve Goodman, Randall F. Springfield and James Hoff reviewed "Building Trusted and Privacy into Open PC Systems," November 2000, Grawrock.

The Grawrock patent discloses the same technology as the Grawrock November 2000 Paper. According to Declaration 1, Grawrock teaches that the verification of the BIOS occurs after it has already been loaded onto the system. Figure 4 in the Grawrock patent also discloses this process whereby identifiers of the boot block, BIOS, BIOS extensions and OS loader are all provided to the TPM for recordation. This is so that a "challenger" may later determine whether the platform should behave in an expected manner for an intended purpose. Grawrock, column 4, lines 36-40. The present invention verifies the authenticity of the BIOS before allowing it to be stored on the flash memory of the system.

Furthermore, there is no language in Grawrock that teaches a TPM performing a signature verification of an update to the program. Instead, Grawrock only teaches providing identifiers of the boot block, BIOS, BIOS extensions and OS loader to the TPM for recordation. There is no signature verification of an update to a program.

Furthermore, claims 1, 4 and 8 specifically recite that the memory unit is unlocked after the verification is successful. According to Declaration 1, Grawrock already stores the updated program, and then performs a TPM verification. Therefore, the Examiner has not presented a *prima facie* case of obviousness in rejecting claims 1, 4 and 8, since the Examiner is relying upon incorrect, factual predicates in support of the rejection. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1455 (Fed. Cir. 1998).

Furthermore, Alexander does not teach these missing claim limitations. Referring to Figure 3A of Alexander, Alexander teaches that the flash memory 212 enters state 330 where flash memory 212 in firmware hub 110 is reset to read/write access. Alexander, column 5, lines 32-34. Flash memory 212 then enters state 332 to check whether there is a valid RBU image to update BIOS 142. Alexander, column 5, lines 34-36. If a valid RBU image exists, flash memory 212 enters state 338 where BIOS 142 updates firmware hub 110 with a new BIOS image and then enters state 302 to load the new image by resetting computer system 100. Alexander, column 5, lines 41-45.

Hence, Alexander teaches that in state 330, the flash memory is reset to a read/write access. This is the same as unlocking the flash memory. Appellants submit herewith the attached Declaration by Steve Goodman, who is attesting to such an assertion ("Declaration 2"). Thereafter, in state 332, Alexander checks whether the RBU image is valid. This is opposite of what the Examiner is asserting.

As a result, Alexander and Grawrock both specifically teach that the flash memory is unlocked before the program is updated. Thus, the combination of

Alexander and Grawrock would install an update to the program, and thereafter verify the program. This is the opposite of what is recited in the claims 1, 4 and 8.

As a result, the combination of Alexander and Grawrock teaches away from the present invention. As a result, the Examiner has failed to provide a *prima facie* case of obviousness in rejecting claims 1, 4 and 8.

Additionally, the Examiner in the Advisory Action cites to column 3, lines 62-64 of Alexander as support for the assertion that Alexander teaches the above-cited claim limitations. Alexander teaches that unlocked blocks can be programmed or erased. Alexander, column 3, line 62. Alexander further teaches that all unlocked blocks return to the locked state when the device is reset or powered down. Alexander, column 3, lines 62-64. Hence, Alexander teaches that unlocked blocks can be programmed or erased and that all unlocked blocks return to the locked state when the device is reset or powered down.

There is no language in the cited passage that teaches a TPM performing a signature verification of an update to a program, as recited in claim 1. Neither is there any language in the cited passage that teaches that if this signature verification is successful, then the TPM unlocks a memory unit to store the program, as recited in claim 1. Neither is there any language in the cited passage that teaches modifying the program with the update to the program in response to the unlocking of the memory unit storing the program, as recited in claim 1. Neither is there any language in the cited passage that teaches a TPM that performs a signature verification of an update to a program, such as a BIOS image, as recited in claims 4 and 8. Neither is there any language in the cited passage that teaches that if this signature verification is successful, then the TPM unlocks a memory unit to store the program, as recited in claims 4 and 8. Neither is there any language in the cited passage that teaches that if the result of the signature verification of the updated BIOS image determines that the updated BIOS image is authentic, then the TPM program unlocks the flash memory

and the BIOS update application modifies the BIOS with the updated BIOS image, as recited in claims 4 and 8.

Thus, for at least the reasons stated above, the combination of Grawrock and Alexander does not teach a TPM performing a signature verification of an update to a program, and then unlocking a memory unit using a TPM for storing the program if the signature verification of the update to the program is successful, and then modifying the program with the update to the program in response to the unlocking of the memory unit storing the program. At the most, the combination of Alexander and Grawrock would install an update to a program and then create identifiers of the update for recordation. Then, a "challenger" can later verify whether the program can be trusted. This is not the same as what is recited in claims 1, 4 and 8.

Therefore, the Examiner has not presented a *prima facie* case of obviousness in rejecting claims 1, 4 and 8, since the Examiner is relying upon incorrect, factual predicates in support of the rejection. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1455 (Fed. Cir. 1998).

2. Claims 2-3, 6-7 and 9-10 are patentable over Alexander in view of Grawrock for at least the reasons that claims 1, 4 and 8, respectively, are patentable over Alexander in view of Grawrock.

Claims 2-3 each recite combinations of features of independent claim 1, and hence claims 2-3 are patentable over Alexander in view of Grawrock for at least the above-stated reasons that claim 1 is patentable over Alexander in view of Grawrock.

Furthermore, claims 6-7 each recite combinations of features of independent claim 4, and hence claims 6-7 are patentable over Alexander in view of Grawrock for at least the above-stated reasons that claim 4 is patentable over Alexander in view of Grawrock.

Additionally, claims 9-10 each recite combinations of features of independent claim 8, and hence claims 9-10 are patentable over Alexander in view of Grawrock for at least the above-stated reasons that claim 8 is patentable over Alexander in view

of Grawrock.

VIII. CONCLUSION

For the reasons noted above, the rejections of claims 1-4 and 6-10 are in error. Appellants respectfully request reversal of the rejections and allowance of claims 1-4 and 6-10.

Respectfully submitted,
WINSTEAD P.C.
Attorneys for Appellants

By: _____
Robert A. Voigt, Jr.
Reg. No. 47,159

P.O. Box 50784
Dallas, Texas 75201
(512) 370-2832

CLAIMS APPENDIX

1. A method for updating a program in a data processing system comprising the steps of:

requesting a trusted platform module ("TPM") to perform a signature verification of an update to the program;

the TPM performing the signature verification of the update to the program;

if the signature verification of the update to the program is successful, using the TPM for unlocking a memory unit storing the program; and

modifying the program with the update to the program in response to the unlocking of the memory unit storing the program.

2. The method as recited in claim 1, further comprising the step of:

locking the memory unit after the modifying step.

3. The method as recited in claim 2, wherein the locking step is performed by the TPM.

4. A computer program product for storage on a computer readable medium and operable for updating a BIOS stored in a flash memory in a data processing system, comprising:

a BIOS update application program receiving an updated BIOS image;

the BIOS update application requesting a TPM to perform a signature verification of the updated BIOS image;

a TPM program receiving the request from the BIOS update application to perform the signature verification of the updated BIOS image;

the TPM program performing the signature verification of the updated BIOS image and posting a result of the signature verification of the updated BIOS image to the BIOS update application;

if the result of the signature verification of the updated BIOS image determines that the updated BIOS image is authentic, then the TPM program unlocks

the flash memory; and

the BIOS update application modifies the BIOS with the updated BIOS image.

6. The computer program product as recited in claim 4, further comprising:

programming for locking the flash memory after the BIOS update application modifies the BIOS with the updated BIOS image.

7. The computer program product as recited in claim 6, further comprising:

if the result of the signature verification of the updated BIOS image determines that the updated BIOS image is not authentic, then an error message is output.

8. A data processing system having circuitry for updating a BIOS stored in a flash memory in the data processing system, comprising:

input circuitry for receiving an updated BIOS image;

circuitry for requesting a TPM to perform a signature verification of the updated BIOS image;

the TPM performing the signature verification of the updated BIOS image;

the TPM unlocking the flash memory if the signature verification of the updated BIOS image determines that the updated BIOS image is authentic; and

circuitry for modifying the BIOS with the updated BIOS image.

9. The system as recited in claim 8, further comprising:

circuitry for locking the flash memory after the BIOS is modified with the updated BIOS image.

10. The system as recited in claim 8, further comprising:

circuitry for outputting an error if the signature verification of the updated BIOS image determines that the updated BIOS image is not authentic.

EVIDENCE APPENDIX

A declaration under 37 C.F.R. §1.132 by Steve Goodman is relied upon by Appellants in the appeal, a copy of which is attached. A declaration under 37 C.F.R. §1.132 by Steve Goodman, Randall F. Springfield and James Hoff is relied upon by Appellants in the appeal, a copy of which is attached.

RELATED PROCEEDINGS APPENDIX

Co-pending U.S. Patent Application Serial No. 09/931,550 has also been appealed by Appellants. That Application is relied upon by the Examiner in his provisional double patenting rejection.

In re Application of: Goodman et al.	:	Before the Examiner: Longbit Chai
Serial No.: 09/931,629	:	Group Art Unit: (not on tape)
Filed: August 16, 2001	:	IBM Corp. Intellectual Property Law
Title: FLASH UPDATE USING A TRUSTED PLATFORM MODULE	:	Dept. 972/B656 P.O. Box 12195 Research Triangle Park, NC 27709

DECLARATION UNDER 37 C.F.R. § 1.132

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

We, Steve Goodman, Randall F. Springfield, and James Hoff, are the inventors of the above-identified Application, and declare as follows:

CERTIFICATION UNDER 37 C.F.R. § 1.8

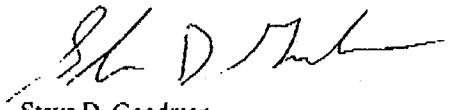
I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on February 14, 2005.

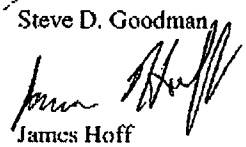
Toni Stanley
Signature

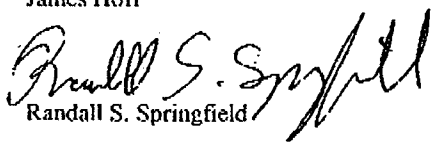
Toni Stanley
(Printed name of person certifying)

1. In the invention as recited in the claims of the above-identified patent application, the trusted platform module ("TPM") is used to do the signature verification of the update to program, and also enables the flash memory to receive the update. This makes the process of putting a tampered update to the program in the flash memory much more difficult.
2. In an example where a TPM does not directly unlock the flash memory unit, there must be a software interface that is used to unlock the flash memory unit, even if signature verification is performed on the program update to be loaded. Once this software interface is understood, it would then be a fairly simple matter of programming to write an application that can unlock the flash memory unit and store anything that is desired within the memory unit.
3. In contrast, within the present invention as claimed, where the TPM directly unlocks the flash memory unit, storing a tampered image (or program update) within the flash memory unit is much more difficult. In addition to figuring out the software interface to unlock the flash memory unit, the person attempting to store a tampered image must also figure out how to fool the TPM into thinking the image and update are authentic. That would mean that such an attacker on the system would have to present both an authentic image and the individual users authentication information to the TPM before the TPM would unlock the flash memory unit. This is significantly harder to do than in the case without using the TPM.
4. *Grawrock* teaches verification of the BIOS image after it has already been stored in the flash memory unit. The present invention verifies the BIOS image before allowing it to be stored in the flash memory unit and unlocking the memory unit.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this Declaration is directed.

By: 
Steve D. Goodman

By: 
James Hoff

By: 
Randall S. Springfield

In re Application of: Goodman et al.	Before the Examiner: Longbit Chai
Serial No.: 09/931,629	Group Art Unit: 2131
Filed: August 16, 2001	Lenovo (United States), Inc. Intellectual Property Law ZHHA/B675/B424 P.O. Box 12195 3039 Cornwallis Road Research Triangle Park, NC 27709
Title: FLASH UPDATE USING A TRUSTED PLATFORM MODULE	

DECLARATION UNDER 37 C.F.R. § 1.132

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

I, Steve Goodman, am an inventor of the above-identified Application, and declare as follows:

Setting flash memory in firmware to read/write access is equivalent to unlocking the flash memory.

CERTIFICATION UNDER 37 C.F.R. § 1.8

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on 10-20, 2005.

Toni Stanley
Signature

Toni Stanley
(Printed name of person certifying)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this Declaration is directed.

By: _____
Steve D. Goodman

P.O. Box 50784
Dallas, Texas 75201
(512) 370-2851